UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,548	09/29/2003	Akira Murakawa	018775-877	7496

21839 7590 11/19/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
GEE, JASON KAI YIN	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
11/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	**Application No.** 10/671,548	**Applicant(s)** MURAKAWA, AKIRA	
	Examiner JASON K. GEE	**Art Unit** 2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _10/09/2009_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-12,17-20,22-24,28,29 and 31-33_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-12,17-20,22-24,28,29 and 31-33_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _19 September 2007_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: RCE filed 10/09/2009.

2. Claims 1-12, 17-20, and 22-24, 28, 29, and 31-33 are currently pending in this application. Claim 30 has been cancelled.

3. No new IDS has been received.

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/09/2009 has been entered.

Response to Arguments

5. In regards to the 112 rejections, these rejections have been withdrawn in response to the arguments presented in 08/03/2009 and also the amendments submitted on 10/09/2009.

6. In regards to the art rejections, applicant's arguments have been fully considered but they are not persuasive.

In regards to the independent claims, the applicant has stated that the Office has “selectively cobbling together bits and pieces of the disclosure of Smetters and disregarding any portion which refutes the Office’s mischaracterization of the actual disclosure of Smetters." However, this is not so. As seen in the rejection below, Smetters clearly teaches everything that the independent claim teaches (such as the creation of two certificates in the same manner, the transfer of the certificates in the same manner, and the verification of the certificates in the same manner), except that the root certificate is preinstalled in a client before the said communication is initiated. As seen in Smetters, the creation of a second/child certificate is created and sent with the original root certificate to a client (paragraphs 31 and 35), and therefore Smetters does not teach wherein the root certificate is already pre-installed in the client. A secondary reference, Benussi was used to teach the limitation wherein root certificates are pre-installed though. This is shown in paragraph 214 of Benussi. As seen here, "each CB [connectivity box] contains in its pre-installed data not only its public key/private key pair, but also the certificate issued by the Root CA [certificate authority] linking the CB public key to the identity of the CB, this identity being the unique serial number of that particular CB." Further, this is also show later in the paragraph: "Finally, to enable a CB to check the authenticity of the certificate sent to it by the CSS ... the public key of the Root CA is pre-installed in each CB as the ' Certificate for Root CA' of parameters." Therefore, as seen in this paragraph, a client (the CB) does indeed have a pre-installed root certificate. This is installed prior to receiving another certificate. The applicants are arguing that only the key is pre-installed, not the certificate. But as paragraph 214 clearly shows, the certificate itself is indeed installed: "each CB contains in its pre-installed data not only its public key/private key pair, **but also the certificate issued by the Root CA**." (emphasis added).

In regards to the independent claims, the applicant also argues that Smetters as modified does not teach that the root certificate is created by the image processing apparatus, and that the second certificate designates the root certificate as a certificate authority at a higher level. However, Smetters clearly teaches this. As seen in paragraph 31, the original laptop 12(1), which is the image processing device, creates the second laptop member certificate. Further, this certificate designates the root certificate as a certificate authority at a higher level. As seen throughout the reference, Smetters disclsoes a chain of certificates (see Figure 7; also paragraph 34, 35). As seen in paragraph 34, the secondary certificates may have limited permissions, such as perhaps not being able to grant access to others. As seen in paragraph 35, the "chain" of certificates is different for each user. For the original root certificate user, laptop 12(1), the certificate chain is merely the root certificate. For a second user, the chain would be the root certificate and the secondary certificate. For a third user, the chain would be the root certificate, the secondary certificate, and the third certificate (Figure 7). As these are chains, each certificate is related, and would designate in some manner that there is a higher certificate. This is further elaborated on in paragraph 45, wherein a secondary member would send the entire chain to a third member, which includes three certificates. Therefore, as these certificate are chained with each other, any certificate under the root certificate would designate that there is a higher “root” certificate that is associated with it (unless it is the root certificate). Sending this chain with all the certificates will definitely designate that a lower certificate is associated with a higher certificate.

7. The applicants also argue the dependent claims as well, which, after further consideration, are not persuasive.

As per claim 10, the applicants argue that the Smetters as modified does not teach wherein the installation of the root certificate is performed after the root certificate is confirmed by a user. However, the applicants are too narrowly interpreting this claim. The claim only limits the action toward "confirming" a root certificate. As seen in paragraph 30 of Smetters, the client indicates that they woudl like to obtain the shared space, and in paragraph 35, the client receives the certificate, and then installs/stores it. There are multiple confirmations taking place here, such as confirming they would like to receive the root certificate, and also confirming that a certificate is received (a certificate must be confirmed that it is received before it can actually be stored/installed). Therefore, Smetters teaches these limitations.

As per claims 20 and 23, as seen, the arguments for the independent claims apply here as well. A taught be Benussi, Benussi teaches that the root certificate and the public key is pre-installed, and thus, the secondary certificate that is sent will be sent after this root certificate is installed.

As per claims 28 and 29, the applicants are arguing that Smetters and Benussi do not teach the features of this claim. However, the Smetters combination clearly teaches these limitations. As seen in Benussi in paragraph 214 (the end of the paragraph), the public key of the root certificate which is pre-installed is used to check the authenticity of the certificate that is later sent to it. Further, Schenier is used to supplement these references to explicitly show that the public keys are used to decrypt information to verify signatures.

8. The applicants also argue that the other dependent claims are allowable for the same reasons as argued above. However, the response to arguments above are applied to these dependent claims as well, and therefore not allowable for the same reasons as indicated above.

Claim Rejections - 35 USC § 112

9. The previous 112 rejections have been withdrawn in response to the arguments presented in 08/03/2009 and also the amendments submitted on 10/09/2009.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 4, 5, 7, 10, 12, 17, 20, 22-24, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters et al. US Patent Application Publication

2004/0088548 (hereinafter Smetters), and in view of Benussi et al. SU Patent Application Publication 2001/0044898 (hereinafter Benussi).

As per claim 1, Smetters teaches a communication system in which an image processing apparatus and a client communicate data with each other through a network, wherein said image processing apparatus comprises (image processing apparatus is laptop 12(1) as seen in paragraph 25): a root certificate creator which creates a root certificate including a public key paired with a private key and being signed with a private key (paragraph 25; also paragraph 26 wherein standard cryptographic authentication techniques are used); a second certificate creator which creates, when a connection for communication is requested by said client, a second certificate (paragraph 28 and 31, wherein the second laptop certificate is created by laptop 12(1) using the same method as the root certificate and sends to client laptop 12(2); the second certificate designating the root certificate created by said root certificate creator as a certificate authority at a higher level and being signed with the private key (paragraphs 34-35, wherein a chain of certificates is created, wherein the original "root certificate" is at the top of the chain; also see paragraphs 44-45, wherein the whole chain must be sent); and a communication device which transmits the second certificate created by said certificate creator to said client (paragraph 35); and wherein said client comprises a storage device which stores the root certificate created by said root certificate creator (paragraph 35); and a verifier which verifies the signature of the second certificate received from said image processing apparatus with the root certificate stored in said second storage device (paragraph 42).

However, at the time of the invention, Smetters does not teach all the limitations of the claims. Smetters does not explicitly teach a storage device which already stored the root certificate before the connection for communication is requested. Smetters in paragraph 35 teaches that the root and the secondary are sent together at the same time. However, it would have been obvious to have stored the root certificate earlier. This is taught in paragraph 214 of Benussi. This paragraph also confirms the standard teachings of signing a certificate with a private key to confirm whether a certificate is genuine or not.

At the time of the invention, it would have been obvious to combine the Smetters and the Benussi reference. One of ordinary skill in the art would have been motivated to perform such an addition to create more security and also providing a system for configuring a connectivity unit that is user friendly and yet involving the provisions of user-specific communication parameters (Benussi paragraph 5).

As per claim 4, Smetters teaches the communication system where the client is a personal computer (paragraph 30).

As per claim 5, Smetters teaches wherein the storage device is a hard disk drive (paragraph 19).

As per claim 7, Smetters teaches a communication method for a communication system in which an image processing apparatus and a client communicate data with each other through a network (paragraph 30, with laptop 12(1) as image processing apparatus and client as laptop 12(2)), wherein the image processing apparatus creates a root certificate including a public key paired with a private key and being signed with the private key (paragraph 25 and 26); the client installs the root certificate which is created by the image processing apparatus which includes the public key (paragraph 31 and 35), the image processing apparatus creates, when a connection for communication is requested by the client (paragraph 28), a second certificate designating the root certificate created by the image processing apparatus as a certificate authority at a higher level and being signed with the private key when data is sent to the client (paragraph 25, 31, 34, 35, 45, wherein the certificates are sent as a chain); the image processing apparatus sends the second certificate to the client (paragraph 35); and the client verifies the signature of the second certificate received from the image processing apparatus with the installed root certificate (paragraph 42).

Smetters does not explicitly teach though that the root certificate is installed in the client before the second certificate is received though. Similar to claim 1, Benussi further shows that it would be obvious to have stored the root certificate earlier before the second certificate is created. This is taught in paragraph 214 of Benussi. This paragraph also teaches and confirms that certificates in general are signed with private keys to confirm whether a certificate is genuine or not.

At the time of the invention, it would have been obvious to combine the Smetters and the Benussi reference. One of ordinary skill in the art would have been motivated to perform such an addition to create more security and also providing a system for configuring a connectivity unit that is user friendly and yet involving the provisions of user-specific communication parameters (Benussi paragraph 5).

As per claim 10, Smetters teaches wherein when the client installs the root certificate, the installation is performed after the root certificate is conformed by a user (paragraph 31).

As per claim 12, Smetters teaches wherein the data is communicated according to the security sockets later (SSL) protocol (paragraph 29).

Claim 17 is rejected using the same basis of arguments used to reject claims 1 and 7 above. Claim 17 is the corresponding system claim. As seen throughout the Smetters reference, the image processing apparatus is laptop 12(1), and the root certificate creators are inside this laptop as it creates the certificates.

As per claim 20, Smetters as modified teaches wherein the root certificate stored in said first storage device is stored in said storage device of said client prior to the transmission of the second certificate from said communication device (Benussi paragraph 214, wherein root certificate is pre-installed in client).

As per claim 22, Smetters teaches wherein said verifier is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in said second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from said device, and compring the first and second hash values to determine if they are equal to each other (paragraph 41 and 42).

As per claim 23, Smetters as modified teaches wherein the image processing apparatus sends the second certificate to the client after the root certificate is installed in the client (Benussi paragraph 214, wherein root certificate is pre-installed in client).

As per claim 24, Smetters discloses wherein the client installs the at least one intermediate certificate prior to receiving the second certificate from the device (paragraph 35).

As per claim 31, Smetters teaches a computer-readable recording medium having a computer program recorded thereon for causing a computing device, which is communicatively coupled to the computer-readable recording medium and which is configured to communicate with a client through a network to send information to the client, which uses the information to communicate with the computing device, to perform operations comprising (paragraph 30, with laptop 12(1), which inherently has programs installed to perform the operations): storing a pair of public key and a private key (paragraph 25); creating a root certificate including the public Key and private key and being signed with the private key (paragraph 25), storing the root certificate signed with the private key (paragraph 25); sending the information and the root certificate created by the computing device and including the public key to the client (paragraph 30, 35); creating, when the connection for communication is requested by the client, a second certificate designating the root certificate created by the computing device as a certificate authority at a higher level and being signed with the private key used to sign the root certificate (paragraph 25, 30, 31, 34, 35, 45, wherein the certificates are sent as a chain); and sending the created second certificate to the client for verification of the information sent from the computing device (paragraph 35).

Smetters does not explicitly teach though that the root certificate is installed in the client before the second certificate is received though. Similar to claim 1 and other independent claims, Benussi further shows that it would be obvious to have stored the root certificate earlier before the second certificate is created. This is taught in paragraph 214 of Benussi. Further, as seen in this paragraph, the public key is in the client before requests for communications have been made as the public key is preinstalled. This paragraph also teaches and confirms that certificates in general are signed with private keys to confirm whether a certificate is genuine or not.

At the time of the invention, it would have been obvious to combine the Smetters and the Benussi reference. One of ordinary skill in the art would have been motivated to perform such an addition to create more security and also providing a system for configuring a connectivity unit that is user friendly and yet involving the provisions of user-specific communication parameters (Benussi paragraph 5).

12. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters and Benussi as applied above, and further in view of Frailong et al. US Patent No. 6,012,100 (hereinafter Frailong).

As per claim 8, Smetters teaches holding at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority (Figure 7); the client installs the at least one intermediate certificate in addition to the root certificate (paragraph 35); the device sends the second certificate to the client (paragraph 31); the client verifies the signature of the second certificate received from the device with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the device with teh root certificate installed therein (paragraph 42).

For further clarification on hierarchical certificates and a device holding the certificates, see Frailong Figure 14 and col. 18 line 55 to col. 19 line 60, wherein a device holds the root certificate along with the intermediate and secondary certificates.

At the time of the invention, it would have been obvious to include the Frailong reference with the Smetters combination. One of ordinary skill in the art would have been motivated to perform such an addition to provide a system for connecting acomputer or client network to the internet with minimal user interaction and also automatically upgrading and reconfiguring a network interface connection between a computer or client network and an internet (col. 2 liens 15-22 of Frailong).

13. Claims 2, 3, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters and Benussi as applied above, and further in view of Debry US Patent No. 6,918,042 (hereinafter Debry).

As per claim 2, the Smetters combination does not teach all the limitations of this claim. However, these deficiencies are taught by Debry. Debry teaches wherein said iamge processing apparatus is a printer (col. 5 lines 59-60).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the teachings of Debry with the Smetters combination. One of ordinary skill in the art would have been motivated to perform such an addition to provide print servers to which computer systems can be communicatively linked (col. 1

lines 5—53) and to protect printers themselves from malicious attacks (col. 5 lines 33-34)..

As per claim 3, the Smetters combination does not teach wherein the said image processing apparatus is a multifunctional peripheral. This is taught by Debry though. Debry teaches wherein the image processing apparatus is a multifunctional peripheral (col. 6 lines 9-14).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the teachings of Debry with the Smetters combination. One of ordinary skill in the art would have been motivated to perform such an addition to provide print servers to which computer systems can be communicatively linked (col. 1 lines 5—53) and to protect printers themselves from malicious attacks (col. 5 lines 33-34)..

Claim 32 is rejected using the same basis of arguments used to reject claim 2 above.

14. Claims 9, 11, 18, 19, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters and Benussi as applied above, and further in view of Debry US Patent No. 6,918,042 (hereinafter Debry) and Slick US Patent Application Publication 2004/0109568 (hereinafter Slick).

With regard to claim 9, Smetters discloses a method comprising: when the client installs the root certificate, the client requests the root certificate from the device ([0031" lines 5-7), receives the root certificate from the device ([0035]: lines 2-'3), converts the received root certificate to a predetermined format when the root certificate is received ([0026]: lines 7-10, since different types of certificates can be used; it is well known in the art for any of these certificates to be converted to one standard in order to communicate with each other), and installs the converted root certificate ([0035]: line 3, storing the certificates in memory reads on client installs the converted root certificate received from the client).

Neither Smetters nor Benussi discloses the device where the device is a printer. Debry, on the other hand, discloses the device is a printer (col. 5: lines 59-60).
It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Smetters and Benussi such that to include the device is a printer, as taught by Debry, and would be motivated to provide print servers to which the computer system can be communicatively linked (col. 1: lines 51-53) and to protect printers themselves from malicious attacks (col. 5: lines 33-34).

However, Smetters, Benussi nor Debry discloses a printer driver from the device is installed in the client device. Slick discloses a printer driver from the device is installed in the client ([0057]: lines 1-4).

At the time of the invention it would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Smetters, Benussi and Debry to include the installation of a printer driver from the device, as taught by Slick, and would be motivated to provide the private key through a printer driver ([0005]: lines 8-11).

As per claim 11, and similar claims 18-19 and 26 - 27, Smetters discloses method/device where the client installs the root certificate after the printer driver from the device is installed in the client ([0035]: line 3, storing the certificates in memory reads on client installs the root certificate received from the client. Furthermore, it is well known in the art for a device to install a driver of that device prior to communicate with it as presented below) but neither Smetters nor Benussi discloses the device is a printer, and install the root certificate after a printer driver is installed from the device.

Debry, on the other hand, discloses the device is a printer (col. 5: lines 59-60). It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Smetters and Benussi such that to include the device that has print function, as taught by Debry, and would be motivated to provide print servers to which the computer system can be communicatively linked (col. 1: lines 51-53) and to protect printers themselves from malicious attacks (col. 5: lines 33-34).

However, Smetters, Benussi nor Debry discloses a printer driver is installed from the device. Slick discloses a printer driver is installed from the device ([0057]: lines 1-4, further notes that in order communication with the printer; the printer driver needs to be active before any communication).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Smetters and Debry such that to include the installation of a printer driver from the device, as taught by Slick and would be motivated to provide the public key through a printer driver ([0005]: lines 8-11).

15. Claim 6 is rejected under 35 USC 103(a) as unpatentable over Smetters and Benussi as applied above, and further in view of Vogel et al. (US Pat. No. 6816900), hereafter "Vogel".

With regard to claim 6, Smetters discloses the communication system (Abstract) but neither Smetters, nor Benussi discloses the second storage device is a read-only memory. Vogel discloses the second storage device is a read-only memory (Fig. 2: item 150).

At the time of the invention, it would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Smetters and Benussi such that to include a read-only memory for the second storage device in the communication system, as taught by Vogel, and would be motivated to provide a more user-friendly way in which root certificates at the client computer can be managed (col. 2: lines 8-10).

16. Claim 28 and 29 are rejected under 35 USC 103(a) as unpatentable over Smetters and Benussi as applied above, and further in Schneier's Applied Cryptography, 2nd Edition (hereinafter Schneier)

As per claims 28, Smetters does not explicitly teach wherein the second storage device of said client has stored therein, before the connection for communication is requested to said device, the public key of the root certificate stored in said first storage device. This is however taught by Benussi in paragraph 214 ("Finally, to enable a CB to check the authenticity of the certificate sent to it by the CSS.. the public key of the Root CA is pre-installed in each CB as the "certificate for Root CA" of parameters." Smetters as modified by Benussi does not explicitly teach how this verification is performed though, such as by verifying the signature of the second certificate received from said device by decrypting the second certificate with the public key of the root certificate stored in said storage device. However, this would have been obvious and is well known. In public key cryptography, public keys are agreed on obtained prior to sending encrypted works, and is used to decrypt certificates with public keys for verification. This is shown in Schenier, in pages 31 and 32. This is also seen in page 37, wherein the stored public key is used to decrypt information and verify the signature.

At the time of the invention, it would have been obvious to combine the Smetters and the Benussi reference. One of ordinary skill in the art would have been motivated to perform such an addition to create more security and also providing a system for configuring a connectivity unit that is user friendly and yet involving the provisions of user-specific communication parameters (Benussi paragraph 5).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the Schenier reference with the Smetters and Benussi combination. One of ordinary skill in the art would have been motivated to include such an addition to create more security. As seen in pages 31 and 32, utilizing such public key algorithms are useful and efficient as they solve the key-management problems with symmetric cryptosystems.

Claim 29 is rejected using the same basis of arguments used to reject claim 27.

17. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters and Benussi as applied above, and further in view of Debry US Patent No. 6,918,042 (hereinafter Debry).

As per claim 32, the Smetters combination does not teach all the limitations of this claim. However, these deficiencies are taught by Debry. Debry teaches wherein a said device is a printer (col. 5 lines 59-60).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the teachings of Debry with the Smetters combination. One of ordinary skill in the art would have been motivated to perform such an addition to provide print servers to which computer systems can be communicatively linked (col. 1 lines 5—53) and to protect printers themselves from malicious attacks (col. 5 lines 33-34)..

18. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smetters and Benussi as applied above, and further in view of Slick US Patent Application Publication 2004/0109568 (hereinafter Slick).

As per claim 33, the Smetters combination does not explicitly teach all the limitations of the claims. However, these deficiences are taught by Slick. Slick teaches discloses a printer driver from the device is installed in the client device. Slick discloses a printer driver from the device is installed in the client ([0057]: lines 1-4).

At the time of the invention it would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Smetters and Benussi to include the installation of a printer driver from the device, as taught by Slick, and would be motivated to provide the private key through a printer driver ([0005]: lines 8-11).

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON K. GEE whose telephone number is (571)272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on (571) 272-38113811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jason Gee/
Patent Examiner
Technology Center 2400
11/10/2009